



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,496	10/29/2001	Carey Nachenberg	20423-05957	3384
34415 7590 04/19/2007 SYMANTEC/ FENWICK SILICON VALLEY CENTER 801 CALIFORNIA STREET MOUNTAIN VIEW, CA 94041			EXAMINER WILLIAMS, JEFFERY L	
			ART UNIT	PAPER NUMBER
			2137	
SHORTENED STATUTORY PERIOD OF RESPONSE		NOTIFICATION DATE	DELIVERY MODE	
3 MONTHS		04/19/2007	ELECTRONIC	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/19/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com  
bhoffman@fenwick.com  
aprice@fenwick.com

**Office Action Summary**

Application No.

10/046,496

Applicant(s)

NACHENBERG ET AL.

Examiner

Jeffery Williams

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 16 February 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-17 and 20-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-17, 20-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>2/16/07</u> . | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

This action is in response to the communication filed on 2/16/07.

All objections and rejections not set forth below have been withdrawn.

***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/16/07 has been entered.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

**Claims 12 – 17 and 30 – 33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** Regarding claims 12 – 17, 30, 32, and 33, they are directed to matter comprised of software per se. As the applicant has not demonstrated that such claimed elements are tangibly embodied,

1 these recitations are held to be nonstatutory. Regarding claim 31, it pertains to a  
2 program embodied by a computer usable medium. As the applicant has not  
3 demonstrated that usable mediums such as carrier waves and signals are not included  
4 within the scope of the claim recitations, this claim is held to be nonstatutory.

5  
6  
7 ***Claim Rejections - 35 USC § 103***

8  
9 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all  
10 obviousness rejections set forth in this Office action:

11 (a) A patent may not be obtained though the invention is not identically disclosed or described as set  
12 forth in section 102 of this title, if the differences between the subject matter sought to be patented and  
13 the prior art are such that the subject matter as a whole would have been obvious at the time the  
14 invention was made to a person having ordinary skill in the art to which said subject matter pertains.  
15 Patentability shall not be negated by the manner in which the invention was made.

16  
17 **Claims 1 – 10 and 12 – 33 rejected under 35 U.S.C. 103(a) as being**  
18 **unpatentable over Bates et al. (Bates), U.S. Patent 6,721,721 B1 in view of**  
19 **Hericourt et al. (Hericourt), U.S. Patent 7,099,916.**

20  
21 Regarding claim 1, Bates et al. discloses:  
22 *entering a first computer virus status mode in response to a first computer virus*  
23 *outbreak report indicating a virus attack threat to a computer network* (Bates et al., col.  
24 1, lines 13-52). Bates et al. reports the outbreak of new and more sophisticated viruses,  
25 and in response, the system of Bates et al. is employed for the purpose of protecting  
26 against these outbreaks.

1        *computing a first computer virus alert time corresponding to entry into the first*  
2        *computer virus status mode* (Bates et al., fig. 7, elem. 214; col. 7, lines 20-35). Herein,  
3        Bates et al. discloses a method for accessing computer content on a local machine or  
4        on a network. Content is filtered based upon a generated virus alert time, a rule derived  
5        from relative time parameters (criterion) entered (via computer means, "computing") by  
6        a user in a virus status mode. The relative time parameters (i.e. "virus found in last 7  
7        days", "not checked in last 14 days") are processed ("computing") into a rule, which is  
8        then utilized by the system to compare with the timestamps of content and make  
9        determinations of trustworthiness (Bates et al., col. 11, lines 12-24; col. 13, lines 22-34;  
10       col. 17, lines 35-49; col. 18, lines 22-30).

11       *comparing a time stamp of a executable computer code with the first computer*  
12       *virus alert time* (Bates et al., col. 9, line 65 – col. 10, line 3; col. 11, lines 12-24; col. 12,  
13       lines 59-62);

14       *and determining the executability of the computer content in response to the*  
15       *result of the comparing step* (Bates et al., col. 9, line 56 – col. 10, line 8; col. 11, lines  
16       12-24). Bates et al. discloses that in response to a comparison, a determination of  
17       computer content executability is performed.

18       Bates discloses that a time stamp of the executable code corresponds, *inter alia*,  
19       to the time the code was virus scanned. However, Bates does not explicitly disclose  
20       that a time stamp of the executable computer code corresponds to an execution time of  
21       the computer code.

1 Hericourt teaches that virus scanning of executable code comprises an execution  
2 of the code (3:25-54).

3 It would have been obvious to one of ordinary skill in the art to recognize  
4 teachings of Hericourt within the system of Bates. This would have been obvious  
5 because one of ordinary skill in the art would have been motivated by the general  
6 teachings of Bates for virus scanning and the teachings of Hericourt for the effective  
7 accomplishment of such.

8  
9 Regarding claim 2, the combination enables:  
10 *receiving a first access control time based on the first virus outbreak report*  
11 (Bates et al., fig. 7, elem. 214). The system of Bates et al. takes human input and  
12 “automatically” generates computer readable parameters.

13 *and converting the first access control time into the first virus alert time* (Bates et  
14 al., fig. 7, elem. 214; col. 12, lines 59-62). A “prior point in time” (“virus alert time”) is  
15 derived from the period of time specified by element 214 (“access control time”) and is  
16 compared to the timestamp of the file.

17  
18 Regarding claim 3, the combination enables:  
19 *wherein the first access control time is a relative time stamp* (Bates et al., fig. 7,  
20 elem. 214; col. 12, lines 59-62). A “prior point in time” (“virus alert time”) is derived from  
21 the period of time specified by element 214 (“access control time”) and is relative in  
22 time.

1

2       Regarding claim 4, the combination enables:

3       *wherein the first access control time is a pre-determined time period for access*  
4       *control under the first computer virus status mode* (Bates et al., fig. 7, elem. 214). The  
5       access control time is pre-determined by the user.

6

7       Regarding claim 5, the combination enables:

8       *determining the presence of a value representing the computer content in a*  
9       *memory table of executable computer content* (Bates et al., col. 7, lines 12-34).

10

11       Regarding claim 6, the combination enables:

12       *wherein the computer content is not executed when the value representing the*  
13       *computer content is not present in the memory table of executable computer content*  
14       (Bates et al., col. 11, lines 11-24; col. 3, lines 24-27). As disclosed by Bates et al.,  
15       content not present in the memory table of executable computer content is flagged as  
16       untrustworthy. The invention as disclosed by Bates et al. is configurable to eliminate  
17       untrustworthy computer content from the list of accessible content, thus not providing  
18       access to the content for execution.

19

20       Regarding claim 7, the combination enables:

21       *wherein the value is a hash value of the computer content* (Bates et al., col. 12,  
22       lines 55-58).

1

2           Regarding claim 8, the combination enables:

3           *wherein the computer content is executed only when the computer content is*  
4 *time stamped prior to the first computer virus alert time* (Bates et al., col. 13, lines 42-  
5 59; col. 3, lines 24-27). Computer content that is time stamped prior to the first  
6 computer virus alert time is branded as trustworthy. Thus, the content would not be  
7 subjected to denial of access for execution.

8

9           Regarding claim 9, the combination enables:

10          *entering types of computer codes that should be blocked from execution in*  
11 *response to the first computer virus outbreak report* (Bates et al., col. 9, line 62 – col.  
12 10, line 28);

13          *and blocking execution of a computer code that belongs to the entered types of*  
14 *computer codes* (Bates et al., col. 3, lines 24-27). The invention as disclosed by the  
15 combination is configurable to eliminate untrustworthy computer content from the list of  
16 accessible content, thus not providing access to the content for execution.

17

18          Regarding claim 10, the combination enables:

19          *generating a second virus alert time in response to a second computer virus*  
20 *outbreak report; comparing the time stamp of the computer content with the second*  
21 *computer virus alert time; determining the executability of the computer content in*  
22 *response to the result of comparing the time stamp of the computer content with the*



1 *second computer virus alert time* (Bates et al., col. 3, lines 5 – 15). The above  
2 limitations of claim 10 are essentially similar to claim 1 with the exception that they are  
3 directed to a second instance of the method of claim 1. The combination enables for  
4 the method of claim 1 produces a set of results. Thus, the combination enables a  
5 secondary instance of the method of claim 1, as the word “set” dictates more than a  
6 singular occurrence of the method of claim 1.

7 *performing antivirus processing upon the computer content* (Bates et al., col. 9,  
8 lines 62-66). The combination enables the processing of computer content for the  
9 likelihood of existing viruses.

10  
11 Regarding claim 12, it is rejected, at least, for the same reasons as claim 1, and  
12 furthermore because the combination enables:

13 *an access control console, for entering a first computer virus status mode in*  
14 *response to receiving a computer virus outbreak report indicating a virus attack threat to*  
15 *a computer network and for recovering a preselected virus access control time*  
16 *corresponding to said virus status mode* (Bates et al., fig. 1, elem. 33; fig. 7);

17 *an anti-virus module, coupled to the access control console, configured to*  
18 *compute a virus alert time based on the virus access control time and to compare a time*  
19 *stamp of a target computer content with the virus alert time prior to execution of the*  
20 *target computer content* (Bates et al., fig. 1, elem. 30; see rejections of claims 1 and 2).

21 *and wherein the anti-virus module is further configured to determine the*  
22 *executability of the computer content in response to comparing the time stamp of the*

1 *target computer content with the virus alert time* (Bates et al., col. 9, line 56 – col. 10,  
2 line 8; col. 11, lines 12-24). The combination enables for in response to a comparison,  
3 a determination of computer content executability is performed. Thus the combination  
4 enables *content executability determination*, comprising an *anti-virus module*, used to  
5 determine the trustworthiness (“executability”) of content.

6  
7 Regarding claim 13, the combination enables:

8 *a memory module for storing time stamps of the plurality of computer contents*  
9 (Bates et al., fig. 1, elem. 46);

10 *and an access control module, coupled to the access control console and to the*  
11 *memory module, for computing the virus alert time and for comparing the time stamp of*  
12 *each target computer content with the virus alert time* (Bates et al., fig. 1, elem. 42; see  
13 rejections of claims 1 and 2).

14  
15 Regarding claim 14, the combination enables:

16 *a computer virus processing module, coupled to the access control module, for*  
17 *further processing a target computer content in order to determine the executability of*  
18 *the target computer content* (Bates et al., fig. 1, elem. 44).

19  
20 Regarding claim 15, the combination enables:

21 *wherein the memory module stores a value representing each of the computer*  
22 *contents* (Bates et al., col. 12, lines 52-65).

1  
2       Regarding claim 16, the combination enables:

3       *wherein the access control module is configured to determine the presence of*  
4 *the value in the memory module as representing a target computer content (Bates et al.,*  
5 *fig. 3).*

6  
7       Regarding claim 17, the combination enables:

8       *wherein the value is a hash value (Bates et al., col. 12, lines 52-65).*

9  
10       Regarding claim 20, it is rejected, at least, for the same reasons as claim 1, and  
11 furthermore because the combination enables:

12       *creating a list of time-stamped executable computer contents (Bates et al., fig. 3,*  
13 *elem. 92).*

14       *entering a virus alert mode in response to a virus outbreak report indicating a*  
15 *virus attack threat to a computer network (Bates et al., fig. 2; col. 1, lines 13-52).*

16       *responsive to the virus alert mode, entering an access control message for*  
17 *specifying an access control rule for blocking the execution of suspicious or susceptible*  
18 *computer contents that are time-stamped not before computed virus alert time, the*  
19 *access control message including a first control parameter for computing the virus alert*  
20 *time (Bates et al., fig. 2; fig. 7; see rejections of claims 1 and 2).*

1        *receiving a request to execute a target computer content; and determining the*  
2        *executability of the target computer content based on the access control rule in the*  
3        *access control message (Bates et al., fig. 2).*

4  
5        Regarding claim 21, the combination enables:  
6        *applying anti-virus operation upon each executable computer content, storing a*  
7        *hash value of each executable computer content in the list; and inserting a time stamp*  
8        *corresponding to the moment of storing the hash value of the executable computer*  
9        *content (Bates et al., fig. 3).*

10  
11       Regarding claim 22, the combination enables:  
12       *receiving the access control message; automatically converting the first control*  
13       *parameter into the virus alert time; comparing the time stamp of the target computer*  
14       *content in the list with the virus alert time; and determining the executability of the target*  
15       *computer content based on the result of the comparing step (Bates et al., fig. 2, fig. 3,*  
16       *fig. 7; see rejections of claims 1 and 2).*

17  
18       Regarding claim 23, the combination enables:  
19       *applying an anti-virus operation upon the target computer content (Bates et al.,*  
20       *fig. 3).*

21  
22       Regarding claim 24, the combination enables:

1           *a second control parameter for specifying types of computer contents that should*  
2   *be subject to the access control rule* (Bates et al., col. 9, line 62 – col. 10, line 28);  
3           *a third control parameter for specifying an expiration time for the access control*  
4   *rule* (Bates et al., fig. 7, elem. 217);  
5           *and a fourth control parameter for identifying the access control message* (Bates  
6   et al., fig. 2).

7  
8           Regarding claim 25, the combination enables:  
9           *determining validity of the access control message based on the third control*  
10   *parameter* (Bates et al., fig. 3);

11  
12           Regarding claim 26, the combination enables:  
13           *determining executability of the target computer content based on the second*  
14   *control parameter* (Bates et al., col. 9, line 62 – col. 10, line 28);

15  
16           Regarding claims 27 and 28, they are rejected for the same reasons as claims 20  
17   and 22, and further because the combination enables the usage of their system in a  
18   network of communicating computers (Bates et al., fig. 1). Communications to a user  
19   can be blocked when computer content is deemed to be untrustworthy (Bates et al., col.  
20   3, lines 24-27, col. 14, line 6 – col. 15, line 8).

21  
22           Regarding claim 29, the combination enables:

1 wherein the data communication is blocked when the target computer content is  
2 time-stamped not before the virus alert time (Bates et al., fig. 3; fig 7).

3  
4 Regarding claim 30, it is rejected, at least, for the same reasons as claim 1, and  
5 furthermore because the combination enables:

6 *a firewall module monitoring data communications initiated by a target computer*  
7 *content and sending a request to examine the data communications* (Bates et al., fig. 1,  
8 *elems.20, 30, 50). The combination enables that the system is useful in a network and*  
9 *it is capable of filtering trustworthy and untrustworthy computer content – thus, acting as*  
10 *a firewall module.*

11 *an access control console, for generating an access control message specifying*  
12 *an access control rule for blocking data communications of the target computer content*  
13 *when said content is time-stamped not before a virus alert time, the access control*  
14 *message including a first control parameter for computing the virus alert time in*  
15 *response to a virus outbreak report indicating a virus attack threat to a computer*  
16 *network* (Bates et al., fig. 7; fig. 2);

17 *and an access control module, coupled to the access control console and the*  
18 *firewall module, configured to receive the access control message and a request from*  
19 *the firewall module, and to compute the virus alert time based on the virus access*  
20 *control time and to determine whether the data communication should be blocked*  
21 *based on the access control rule* (Bates et al., fig. 1, elem. 44, see rejections of claims 1  
22 *and 2).*

1

2       Regarding claim 31, it is a program and computer medium claim implementing  
3 the method claim 1, and it is rejected for the same reasons (see also, Bates et al., fig.  
4 1).

5

6       Regarding claim 32, it is rejected, at least, for the same reasons as claim 1, and  
7 furthermore because the combination enables:

8       *means for entering a computer virus status mode in response to a virus outbreak*  
9 *report indicating a virus attack threat to a computer network and for automatically*  
10 *recovering a preselected virus access control time (Bates et al., fig. 7);*

11       *coupled to the entering and recovering means, means for computing a virus alert*  
12 *time based on the virus access control time (Bates et al., fig. 1, elems. 31, 42, 44),*  
13 *and coupled to the computing virus alert time means, means for comparing a*  
14 *time stamp of a target computer content with the virus alert time prior to execution of the*  
15 *computer content (Bates et al., fig. 1, elem. 42),*

16       *and for determining the executability of the computer content in response to*  
17 *comparing the time stamp of the target computer content with the virus alert time (Bates*  
18 *et al., col. 9, line 56 – col. 10, line 8; col. 11, lines 12-24). The combination enables a*  
19 *determination of computer content executability is performed for determining the*  
20 *trustworthiness ("executability") of content.*

21

1           Regarding claim 33, it is rejected, at least, for the same reasons as claim 1, and  
2           furthermore because The combination enables:

3           *means for storing time-stamped executable computer contents* (Bates et al., fig.  
4           1, elem. 46);

5           *a firewall means for monitoring data communications occurring to the executable*  
6           *computer contents* (Bates et al., fig. 1, elems. 44, 29, 52).

7           *means for entering a computer virus status mode in response to a virus outbreak*  
8           *report indicating a virus attack threat to a computer network and for automatically*  
9           *recovering a preselected virus access control time* (Bates et al., fig. 7);

10          coupled to the entering and recovering means, means for computing a virus alert  
11          time based on the virus access control time (*Bates et al., fig. 1, elems. 31, 42, 44*).

12          *and coupled to the computing virus alert time means, the storing means, and the*  
13          *firewall means, means for comparing a time stamp of an executable computer content*  
14          *with the virus alert time to determine whether the data communication occurring to the*  
15          *executable computer content should be blocked* (Bates et al., fig. 1, elem. 44, 42).

16  
17  
18          **Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over the**  
19          **combination of Bates et al. and Hericourt in view of Symantec, "Norton AntiVirus**  
20          **Corporate Edition".**

21  
22          Regarding claim 11, The combination enables that viruses can be found in email  
23          attachments, and that it is well known in the art for antivirus programs to have the



1 capability for performing antivirus processing on emails and email attachments (Bates et  
2 al., col. 1, lines 35-63). The combination enables an antivirus program or module for  
3 performing such antivirus processing (Bates et al., fig. 1, elems. 44, 52). Bates et al.,  
4 however, does not disclose the details of the antivirus processing for emails and email  
5 attachments. Specifically, Bates et al. does not disclose that the antivirus program or  
6 module removes the computer content from the E-mail body, and denies execution of  
7 the computer content.

8 Symantec discloses an antivirus program and the details of how the program  
9 performs antivirus processing upon an email with an attachment. Symantec discloses  
10 that the antivirus program scans content attached to an email body and removes such  
11 content if it is found to contain a virus, thus, denying execution of the content  
12 (Symantec, page 15, par. 2; page 22, "Managing Realtime Protection").

13 It would have been obvious for one of ordinary skill in the art to combine the  
14 details disclosed by Symantec for the antivirus processing of emails with the system of  
15 Bates et al. because the system of The combination enables an antivirus program  
16 capable of performing antivirus processing for processing of emails.

17  
18  
19 ***Response to Arguments***

20  
21 Applicant's arguments with respect to the rejected claims above have been  
22 considered but are moot in view of the new ground(s) of rejection.

**Conclusion**

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

**See Notice of References Cited**

A shortened statutory period for reply is set to expire 3 months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Art Unit: 2137

1 Information regarding the status of an application may be obtained from the  
2 Patent Application Information Retrieval (PAIR) system. Status information for  
3 published applications may be obtained from either Private PAIR or Public PAIR.  
4 Status information for unpublished applications is available through Private PAIR only.  
5 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should  
6 you have questions on access to the Private PAIR system, contact the Electronic  
7 Business Center (EBC) at 866-217-9197 (toll-free).

8  
9  
10 Jeffery Williams  
11 AU: 2137  
12

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER